Interference 8 updated Serial 10/752,665

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	watermark$3.clm. and embed$4.clm. and information.clm. and codeword.clm. and collusion.clm. and attack.clm. and target.clm. and "N-1".clm.	USPAT	OR	OFF	2006/02/25 14:55
L2	0	watermark$3.clm. and embed$4.clm. and information.clm. and codeword.clm. and collusion.clm. and attack.clm. and target.clm. and "N-1".clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/25 14:55
L3	2	watermark$3.clm. and embed$4.clm. and information.clm. and codeword.clm. and collusion.clm. and attack.clm. and target.clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/25 14:59
L4	2271	713/176	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/25 14:56
L5	2450	283/13 or 382/276 or 705/75 or 382/308	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/25 14:56
L6	4581	5 or 4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/25 14:56
L7	1	6 and 3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/25 14:56
L8	3	watermark$3 and embed$4 and information and codeword and collusion and attack and target and "N-1"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/25 15:00

EAST Search History

L9	4	watermark$3 and embed$4 and information and codeword and collusion and attack and target	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/25 15:00
L10	4	9 or 3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/25 15:00
L11	3	10 and 6	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/02/25 15:01

10/752,665 NPL

PORTAL USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: The ACM Digital Library The Guide

watermark$3 and embed$4 and information and codeword and

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **watermark$3** and **embed$4** and **information** and **codeword** and **collusion** and **attack** and **target** and **1**

Found **7,251** o **171,14**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Session 7C: Lower bounds for collusion-secure fingerprinting

Chris Peikert, Abhi shelat, Adam Smith

January 2003 **Proceedings of the fourteenth annual ACM-SIAM symposium on Discrete algorithms**

Publisher: Society for Industrial and Applied Mathematics

Full text available: pdf(832.32 KB) Additional Information: full citation, abstract, references, citings, index terms

Collusion-secure fingerprinting codes are an important primitive used by many digital watermarking schemes [1, 10, 9]. Boneh and Shaw [3] define a model for these types of codes and present an explicit construction. Their code has length $O(c^3 \log(l/\varepsilon))$ and attains security against coalitions of size c with ε error. Boneh and Shaw also present a lower bound of $\Omega(c^3 \log(1/c\varepsilon))$ on the length of any collusion-secu ...

2 Session 3A: Optimal probabilistic fingerprint codes

Gábor Tardos

June 2003 **Proceedings of the thirty-fifth annual ACM symposium on Theory of computing**

Publisher: ACM Press

Full text available: pdf(254.76 KB) Additional Information: full citation, abstract, references, index terms

We construct binary codes for fingerprinting. Our codes for n users that are ε-secure against c pirates have length $O(c^2 \log(n/\varepsilon))$. This improves the codes proposed by Boneh and Shaw [3] whose length is approximately the square of this length. Our codes are probabilistic. By proving matching lower bounds we establish that the length of these codes is best within a constant factor for reasonable error probabilities. This lower bound generalizes the ...

Keywords: collusion-secure codes, cryptography, fingerprint

3 New constructions for multicast re-keying schemes using perfect hash families

Rei Safavi-Naini, Huaxiong Wang

November 2000 **Proceedings of the 7th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(384.70 KB) Additional Information: full citation, references, citings, index terms

Keywords: broadcast encryption, perfect hash family, secure multicasting

4 Asymmetric fingerprinting for larger collusions

Birgit Pfitzmann, Michael Waidner

April 1997 **Proceedings of the 4th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(1.37 MB) Additional Information: full citation, references, citings, index terms

5 Fingerprinting: Building efficient and effective multimedia fingerprints via joint coding and embedding

Shan He, Min Wu

August 2005 **Proceedings of the 7th workshop on Multimedia and security MM&Sec '05**

Publisher: ACM Press

Full text available: pdf(594.32 KB) Additional Information: full citation, abstract, references, index terms

Digital fingerprinting protects multimedia content from illegal redistribution by uniquely marking every copy of the content distributed to each user. One major category of collusion-resistant fingerprinting employs an explicit step of coding. Most existing works on coded fingerprinting mainly focus on the code-level issues and treat the embedding issues through abstract assumptions without examining the overall performance. In this paper, we jointly consider the coding and embedding issues for ...

Keywords: collusion resistance, error correcting code, multimedia fingerprinting

6 Session 7: content watermarking: Multimedia content screening using a dual watermarking and fingerprinting system

Darko Kirovski, Henrique Malvar, Yacov Yacobi

December 2002 **Proceedings of the tenth ACM international conference on Multimedia**

Publisher: ACM Press

Full text available: pdf(262.42 KB) Additional Information: full citation, abstract, references, citings

We present a new dual watermarking and fingerprinting system, where initially all copies of a protected object are identically watermarked using a secret key, but individual detection keys are distinct. By knowing a detection key, an adversary cannot recreate the original content from the watermarked content. However, knowledge of any one detection key is sufficient for modifying the object so that a detector using that key would fail to detect the marks. Detectors using other detection keys wou ...

7 Supporting cryptographic technology: New traitor tracing schemes using bilinear map

V. D. Tô, R. Safavi-Naini, F. Zhang

October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management DRM '03**

Publisher: ACM Press

Full text available: pdf(226.82 KB) Additional Information: full citation, abstract, references, index terms

Mitsunari et al [15] presented a new traitor tracing scheme which uses Weil pairing in elliptic curves. To the best of our knowledge this is the first scheme that uses bilinear map. The claimed advantage of the scheme is that the ciphertext size is independent of the number of traitors. It is shown that the problem of constructing a pirate key by *k* colluders

is as hard as the so-called "*k*-weak Diffie-Hellman problem".In this paper, we show an attack on this scheme in which traitors ...

Keywords: bilinear map, elliptic curve, revocation, traitor tracing

8 Anonymous credit cards and their collusion analysis
Steven H. Low, Nicholas F. Maxemchuk, Sanjoy Paul
December 1996 **IEEE/ACM Transactions on Networking (TON)**, Volume 4 Issue 6
Publisher: IEEE Press
Full text available: pdf(860.04 KB) Additional Information: full citation, references, citings, index terms

9 Cryptography: Password authenticated key exchange using hidden smooth subgroups
Craig Gentry, Philip Mackenzie, Zulfikar Ramzan
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press
Full text available: pdf(300.13 KB) Additional Information: full citation, abstract, references, index terms

Existing techniques for designing efficient password authenticated key exchange (PAKE) protocols all can be viewed as variations of a small number of fundamental paradigms, and all are based on either the Diffie-Hellman or RSA assumptions. In this paper we propose a new technique for the design of PAKE protocols that does not fall into any of those paradigms, and which is based on a different assumption. In our technique, the server uses the password to construct a multiplicative group with a (h ...

Keywords: authentication, cryptography, key exchange, password

10 Anonymous authentication with subset queries (extended abstract)
Dan Boneh, Matt Franklin
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(613.93 KB) Additional Information: full citation, abstract, references, citings, index terms

We develop new schemes for anonymous authentication that support identity escrow. Our protocols also allow a prover to demonstrate membership in an arbitrary subset of users; key revocation is an important special case of this feature. Using the Fiat-Shamir heuristic, our interactive authentication protocols yield new constructions for non-interactive group signature schemes. We use the higher-residuosity assumption, which leads to greater efficiency and more natural security proofs than pr ...

Keywords: anonymous authentication, group signature, identity escrow

11 Peer-to-peer infrastructure: Secure routing for structured peer-to-peer overlay networks
Miguel Castro, Peter Druschel, Ayalvadi Ganesh, Antony Rowstron, Dan S. Wallach
December 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue SI
Publisher: ACM Press
Full text available: pdf(1.99 MB) Additional Information: full citation, abstract, references

Structured peer-to-peer overlay networks provide a substrate for the construction of large-

scale, decentralized applications, including distributed storage, group communication, and content distribution. These overlays are highly resilient; they can route messages correctly even when a large fraction of the nodes crash or the network partitions. But current overlays are not secure; even a small fraction of malicious nodes can prevent correct message delivery throughout the overlay. This problem ...

12 Applied cryptography: Reusable cryptographic fuzzy extractors

Xavier Boyen

October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(251.61 KB) Additional Information: full citation, abstract, references, index terms

We show that a number of recent definitions and constructions of fuzzy extractors are not adequate for multiple uses of the same fuzzy secret---a major shortcoming in the case of biometric applications. We propose two particularly stringent security models that specifically address the case of fuzzy secret reuse, respectively from an outsider and an insider perspective, in what we call a chosen perturbation attack. We characterize the conditions that fuzzy extractors need to satisfy to be sec ...

Keywords: biometric keying, chosen perturbation security, fuzzy extractor, zero storage biometric authentication

13 Security-control methods for statistical databases: a comparative study

Nabil R. Adam, John C. Worthmann

December 1989 **ACM Computing Surveys (CSUR)**, Volume 21 Issue 4

Publisher: ACM Press

Full text available: pdf(3.64 MB) Additional Information: full citation, abstract, references, citings, index terms, review

This paper considers the problem of providing security to statistical databases against disclosure of confidential information. Security-control methods suggested in the literature are classified into four general approaches: conceptual, query restriction, data perturbation, and output perturbation. Criteria for evaluating the performance of the various security-control methods are identified. Security-control methods that are based on each of the four approaches are discussed, t ...

14 Key establishment in sensor networks: Location-aware key management scheme for wireless sensor networks

Dijiang Huang, Manish Mehta, Deep Medhi, Lein Harn

October 2004 **Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks**

Publisher: ACM Press

Full text available: pdf(315.08 KB) Additional Information: full citation, abstract, references, index terms

Sensor networks are composed of a large number of low power sensor devices. For secure communication among sensors, secret keys must be established between them. Recently, several pairwise key schemes have been proposed for large distributed sensor networks. These schemes randomly select a set of keys from a key pool and install the keys in the memory of each sensor. After deployment, the sensors can set up keys by using the preinstalled keys. Due to lack of tamper-resistant hardware, the sen ...

Keywords: key management, probabilistic key sharing, sensor networks

15 Pseudonyms and data privacy: The pynchon gate: a secure method of pseudonymous

mail retrieval
Len Sassaman, Bram Cohen, Nick Mathewson
November 2005 **Proceedings of the 2005 ACM workshop on Privacy in the electronic society WPES '05**
Publisher: ACM Press
Full text available: pdf(306.60 KB) Additional Information: full citation, abstract, references, index terms

We describe the Pynchon Gate, a practical pseudonymous message retrieval system. Our design uses a simple distributed-trust private information retrieval protocol to prevent adversaries from linking recipients to their pseudonyms, even when some of the infrastructure has been compromised. This approach resists global traffic analysis significantly better than existing deployed pseudonymous email solutions, at the cost of additional bandwidth. We examine security concerns raised by our model, and ...

Keywords: anonymity, mix networks, private information retrieval

16 Marking and tracing methods: Traitor tracing for prerecorded and recordable media
Hongxia Jin, Jeffery Lotspiech, Stefan Nusser
October 2004 **Proceedings of the 4th ACM workshop on Digital rights management**
Publisher: ACM Press
Full text available: pdf(188.04 KB) Additional Information: full citation, abstract, references, index terms

In this paper we are focusing on the use of a traitor tracing scheme for distribution models that are based on prerecorded or recordable physical media. When a pirated copy of the protected content is observed, the traitor tracing scheme allows the identification of at least one of the real subscribers who participated in the construction of the pirated copy. We show how we systematically assign the variations to users. We explore under what circumstances traitor tracing technology is applica ...

Keywords: content protection, security, traitor tracing

17 Scheduling and resource allocation: SHARP: an architecture for secure resource peering
Yun Fu, Jeffrey Chase, Brent Chun, Stephen Schwab, Amin Vahdat
October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**
Publisher: ACM Press
Full text available: pdf(339.51 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper presents Sharp, a framework for secure distributed resource management in an Internet-scale computing infrastructure. The cornerstone of Sharp is a construct to represent cryptographically protected resource <it>claims</it>---promises or rights to control resources for designated time intervals---together with secure mechanisms to subdivide and delegate claims across a network of resource managers. These mechanisms enable flexible <it>resource peeri ...

Keywords: peer-to-peer, resource allocation, resource peering

18 Watermarking: Improved watermark detection for spread-spectrum based watermarking using independent component analysis
Hafiz Malik, Ashfaq Khokhar, Rashid Ansari
November 2005 **Proceedings of the 5th ACM workshop on Digital rights management DRM '05**

Publisher: ACM Press
Full text available: pdf(434.70 KB) Additional Information: full citation, abstract, references, index terms

This paper presents an efficient blind watermark detection/decoding scheme for spread spectrum (SS) based watermarking, exploiting the fact that in SS-based embedding schemes the embedded watermark and the host signal are mutually independent and obey non-Gaussian distribution. The proposed scheme employs the theory of independent component analysis (ICA) and posed the watermark detection as a blind source separation problem. The proposed ICA-based blind detection/decoding scheme has been simula ...

Keywords: blind source separation, correlation, detection, independent component analysis, spread spectrum, watermarking

19 Networks I: The effect of communication costs in solid-state quantum computing architectures

Dean Copsey, Mark Oskin, Tzvetan Metodiev, Frederic T. Chong, Isaac Chuang, John Kubiatowicz

June 2003 **Proceedings of the fifteenth annual ACM symposium on Parallel algorithms and architectures**

Publisher: ACM Press
Full text available: pdf(149.00 KB) Additional Information: full citation, abstract, references, index terms

Quantum computation has become an intriguing technology with which to attack difficult problems and to enhance system security. Quantum algorithms, however, have been analyzed under idealized assumptions without important physical constraints in mind. In this paper, we analyze two key constraints: the short spatial distance of quantum interactions and the short temporal life of quantum data.In particular, quantum computations must make use of extremely robust error correction techniques to exten ...

Keywords: quantum architecture, quantum computing, silicon-based quantum computing

20 RDS: Remote Distributed Scheme for Protecting Mobile Agents

Asnat Dadon-Elichai

July 2004 **Proceedings of the Third International Joint Conference on Autonomous Agents and Multiagent Systems - Volume 1**

Publisher: IEEE Computer Society
Full text available: pdf(202.70 KB) Additional Information: full citation, abstract, index terms

As of today no software-only based solution that prevents tampering of the computation of any mobile code and/or agent was presented. It is currently accepted that such a solution cannot be supported unless a minimal trust with an honest third party is provided. This paper shows that under very mild assumptions, there exists such a solution that does not base on this trust assumption. A novel Remote Distributed Scheme (RDS) is described. RDS is based on fault-tolerant and modest cryptographic te ...

Keywords: Security, mobile agents, secret - sharing

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2006 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player